CLAIMS

What is claimed is:

1. A method for detecting possible security violations and issues in a computer system related to user ID substituting and switching, said computer system having a log of user ID substitutions and switches, said method comprising the steps of:

providing a set of rules which define conditions of user ID substitutions and switches which are to be considered possible security issues;

providing a process adapted to evaluate said log of user ID substitutions and switches according to said set of rules;

evaluating said log of user ID substitutions and switches to find any entries in said log which meet one or more defined conditions in said set of rules; and

outputting an alert responsive to finding one or more log entries which meet said conditions.

2. The method as set forth in Claim 1 wherein said step of providing a process adapted to evaluate said log comprises configuring a script to periodically execute by a CRON daemon in a system having a UNIX-like operating system.

3. The method as set forth in Claim 1 wherein said step of providing a process adapted to evaluate said log comprises configuring a process to periodically

execute by a CRON daemon in a system having a UNIX-like operating system.

4. The method as set forth in Claim 1 wherein said step of evaluating said log of user ID substitutions and switches comprises evaluating a SULOG file in a system having a UNIX-like operating system.

5. The method as set forth in Claim 1 wherein said step of outputting an alert comprises sending an electronic message to a predetermined destination address.

6. A computer-readable medium having stored therein program code for detecting possible security violations and issues in a computer system related to user ID substituting and switching, said computer system having a log of user ID substitutions and switches, said program code when executed by a computer system causing the computer system to perform the steps of:

providing a set of rules which define conditions of user ID substitutions and switches which are to be considered possible security issues;

evaluating said log of user ID substitutions and switches to find any entries in said log which meet one or more defined conditions in said set of rules; and

outputting an alert responsive to finding one or more log entries which meet said conditions.

7. The computer readable medium as set forth in Claim 6 wherein said program code for performing the step of evaluating said log comprises program code

for configuring a script to periodically execute by a CRON daemon in a system having a UNIX-like operating system.

8. The computer readable medium as set forth in Claim 6 wherein said program code for performing the step of evaluating said log comprises program code for configuring a process to periodically execute by a CRON daemon in a system having a UNIX-like operating system.

9. The computer readable medium as set forth in Claim 6 wherein said program code for performing the step of evaluating said log of user ID substitutions and switches comprises program code for evaluating a SULOG file in a system having a UNIX-like operating system.

10. The computer readable medium as set forth in Claim 6 wherein said program code for performing the step of outputting an alert comprises program code for sending an electronic message to a predetermined destination address.

11. A system for detecting possible security violations and issues in a multi-user computer related to user ID substituting and switching, said multi-user computer having a log of user ID substitutions and switches, said system comprising:

a set of rules which define conditions of user ID substitutions and switches which are to be considered possible security issues;

a log evaluator for evaluation said log of user ID substitutions and switches to find any entries in said log which meet one or more defined conditions in said set of rules; and

an alert output for outputting an alert responsive to finding one or more log entries which meet said conditions.

12. The system as set forth in Claim 11 further comprising a scheduler for periodically operating said log evaluator.

13. The system set forth in Claim 12 wherein said scheduler comprises a CRON daemon and said log evaluator comprises a script in a multi-user computer having a UNIX-like operating system.

14. The system as set forth in Claim 12 wherein said scheduler comprises a CRON daemon and said evaluator comprises an executable UNIX process in a multi-user computer having a UNIX-like operating system.

15. The system as set forth in Claim 11 wherein said evaluator is adapted to evaluate an SULOG file in a multi-user computer system having a UNIX-like operating system.

16. The system as set forth in Claim 11 wherein said alert output comprises a transmitter for an electronic message to a predetermined destination address.